

## UNITED STATES DISTRICT COURT

for the  
District of New MexicoFILED  
U.S. DISTRICT COURT  
DISTRICT OF NEW MEXICO  
2018 SEP -6 PM 1:55  
CLERK-LAS CRUCES

In the Matter of the Search of

*(Briefly describe the property to be searched  
or identify the person by name and address)*A Lenovo IdeaPad Laptop Computer Serial Number  
R8-GMWH7, Currently in the Possession of the FBI

Case No. 18MR851

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, hereby incorporated by reference.

located in the \_\_\_\_\_ District of \_\_\_\_\_ New Mexico \_\_\_\_\_, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, hereby incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. § 2252A(a)(5)

Knowing Possession of Child Pornography

18 U.S.C. § 2252A(a)(2)

Knowing Receipt and Distribution of Child Pornography

The application is based on these facts:

See Affidavit in Support of Warrant, which is hereby incorporated by reference.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
 Applicant's signature

Special Agent Lisa Kite Hill, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 6 Sep 2018

  
 Judge's signature

City and state: Las Cruces, New Mexico

Gregory B. Wormuth, United States Magistrate Judge

Printed name and title

**ATTACHMENT A**

PROPERTY TO BE SEARCHED

The property to be searched is a black Lenovo IdeaPad laptop computer bearing serial number: R8-GMWH7, Product ID: 4187RWU (hereinafter the "Device"). The Device is located at the Federal Bureau of Investigations Las Cruces, Evidence Room, 2509 N. Telshor Boulevard, Las Cruces, New Mexico.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

*Handwritten signature/initials in blue ink.*

## ATTACHMENT B

### ITEMS TO BE SEIZED

1. All items to be seized are evidence, contraband, fruits, and/or instrumentalities of violations of 18 U.S.C. and evidence of crimes constituting violations of Title 18 U.S.C. § 2252A(a)(2) (receipt and distribution of child pornography) and 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography), namely:

- a. Child pornography, as defined in 18 U.S.C. § 2256(8).
- b. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer to child pornography, as defined in 19 U.S.C. § 2256(8), including but not limited to, documents that refer to the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography.
- c. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography, as defined in 18 U.S.C. § 2256(8).
- d. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(B).



- e. Any records, documents, programs, applications, materials, or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques for child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.
- f. Any records, documents, programs, applications, or materials, including electronic messages, that pertain to peer-to-peer file-sharing software.
- g. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to accounts with any Internet Service Provider.
- h. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession of the digital device, which was located within an office inside the Observatory known as the Dunn Solar Telescope, Sunspot, New Mexico on August 21, 2018.
- i. Any digital device used to facilitate the above-listed violations and forensic copies thereof.
- j. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized;

- i. Evidence of who used, owned or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;
- ii. Evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- iii. Evidence of the attachment of other devices;
- iv. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device.
- v. Evidence of the times the device was used;
- vi. Passwords, encryption keys, and other access devices that may be necessary to access the device;
- vii. Applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;
- viii. Records of or information about Internet Protocol addresses used by the device;

- ix. Records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras, peripheral input/output devices, such as keyboards, printers, scanners plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

UNITED STATES DISTRICT COURT

DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF: }  
A Lenovo IdeaPad Laptop Computer Serial }  
Number R8-GMWH7, Currently in the }  
Possession of the Federal Bureau of }  
of Investigation }

Case No. \_\_\_\_\_

**AFFIDAVIT IN SUPPORT OF AN APPLICATION**

**UNDER RULE 41 FOR A SEARCH WARRANT**

I, Lisa Kite Hill, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent with the Federal Bureau of Investigation (FBI). I have been a Special Agent with the FBI since August of 2003. I am classified, trained, and employed as a federal law enforcement officer with statutory arrest authority charged with conducting criminal investigations of alleged violations of federal criminal statutes, including Title 18 of the United States Code. I am currently assigned as a criminal investigator for the Albuquerque Field Office, Las Cruces Resident Agency, New Mexico. Prior to my current position, I investigated fraud, public corruption, and violent crimes against children for twelve years at the Washington Field Office, Washington, D.C. Prior to being a Special Agent of the FBI, I was a healthcare administrator for over ten years. During my tenure with the FBI, I have received formal and informal training in conducting a variety of criminal investigations, including the investigation of individuals involved in the exploitation of minors including violations of Title 18, United States Code, Sections 2251, 2252, and 2252A. I have worked dozens of child pornography and child enticement investigations and have been trained in the investigation of computer related child

exploitation and child pornography cases. During the investigation of these cases, I have executed, or participated in the execution of over forty search warrants and seized evidence of these violations. I have utilized investigative techniques including, but not limited to, consensual monitoring, witness and subject interviews, and online undercover operations.

2. I am investigating the activities of an individual who is utilizing the wireless internet service within the National Solar Observatory in Sunspot, New Mexico, to download and distribute child pornography. As will be shown below, there is probable cause to believe that someone using the wireless internet service within the Observatory was utilizing software to receive, possess, or distribute child pornography, in violation of 18 U.S.C. §§2252 and 2252A. I submit this application and affidavit in support of a search warrant authorizing a search of the digital device as further described in Attachment A. Located with the digital device to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations, which relate to knowing transportation, shipment, receipt, possession, distribution, and reproduction of child pornography. I request authority to search the entire digital device, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

3. The statements in this affidavit are based in part on information provided by New Mexico Internet Crimes Against Children (NM ICAC) Special Agents Owen Pena and Jay Ratliff and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, United States Code §§2252 and 2252A, are presently located within the Lenovo IdeaPad Laptop Computer, Serial Number: R8-GMWH7, which is currently located in the evidence room of the

Federal Bureau of Investigation, and which was seized by your affiant from the National Solar Observatory in Sunspot, New Mexico.

#### **STATUTORY AUTHORITY**

4. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252, and 2252A, relating to material involving the sexual exploitation of minors. Based upon my training and experience, as well as conversations with other experienced law enforcement officers, federal prosecutors, and computer forensic examiners, I know the following:

a. 18 U.S.C. § 2252(a) in pertinent part prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing or accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct using any means or facilities of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mails.

b. 18 U.S.C. § 2252A(a) in pertinent part prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any child pornography, as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer.

c. 18 U.S.C. § 2252(a)(1) prohibits a person from knowingly transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mails, any visual depiction of minors engaging in sexually explicit conduct. Under 18 U.S.C. § 2252(a)(2), it is a federal crime for any person to knowingly receive or distribute, by any means including by computer, any visual depiction of minors engaging in sexually explicit conduct using any means or facility of interstate or foreign commerce

or that has been mailed or shipped or transported in or affecting interstate or foreign commerce. That section also makes it a federal crime for any person to knowingly reproduce any visual depiction of minors engaging in sexually explicit conduct for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails. Under 18 U.S.C. § 2252(a)(4), it is also a crime for a person to knowingly access with intent to view, one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in and affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer.

d. 18 U.S.C. § 2252A(a)(1) prohibits a person from knowingly mailing, transporting, or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including a computer.

#### **DEFINITIONS**

5. The following definitions apply to this Affidavit:

a. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as used here, includes the definitions in 18 U.S.C. §§ 2256(8) and 2256(9) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction was a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct). See U.S.C. §§ 2252 and 2256(2).

c. "Visual depictions" include undeveloped film and videotape, and data stored on a computer disk or by electronic means which is capable of conversion into a visual image, and which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in permanent format. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. "Computer," as used herein, is defined pursuant 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device

performing logical, arithmetic or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”

f. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing), or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard

disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

i. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Digitally coded data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

k. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

1. "Peer-to-peer file-sharing" ("P2P") is a method of communication available to Internet users through the use of special software. Computers or cellular telephones linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer or cellular telephone to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer or cellular telephone, and conducting searches for files that are currently being shared on another user's computer.

### **COMPUTERS AND CHILD PORNOGRAPHY**

6. Based upon my training and experience, as well as conversations with other experienced law enforcement officers and computer forensic examiners, I know that computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. In the past, child pornography was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images, and to distribute these images on any scale required significant resources and significant risks. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public and/or law enforcement. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

7. The development has radically changed the way that child pornographers obtain, distribute and store their contraband. Computers basically serve five functions in connection with child pornography: access, production, communications, distribution, and storage.

8. Child pornographers can now convert paper photographs taken with a traditional camera (using ordinary film) into a computer readable format with a device known as a scanner. Moreover, with the advent, proliferation and widespread use of digital cameras, the images can now be transferred directly from a digital camera onto a computer using a connection known as a USB cable or other device. Digital cameras have the capacity to store images and videos indefinitely, and memory storage cards used in these cameras are capable of holding hundreds of images and videos. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

9. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media, that is, the hard disk drive used in home computers has grown tremendously within the last several years. These hard disk drives can store hundreds of thousands of images at very high resolution.

10. The World Wide Web of the Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

11. Collectors and distributors of child pornography frequently use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Hotmail, Apple Inc., and Google, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer or cellular telephone with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer or cellular telephone. Even in cases where

online storage is used, however, evidence of child pornography can be found on the user's computer or cellular telephone in most cases.

12. As is the case with most digital technology, communication by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving particular website locations in, for example, "bookmarked" files. Digital information, images and videos can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files of ISP client software, among others). Often, a computer will automatically save transcripts of logs of electronic communications between its user and other users that have occurred over the Internet. These logs are commonly referred to as "chat logs." Some programs allow computer users to trade images while simultaneously engaging in electronic communications with each other. This is often referred to as "chatting," or "instant messaging."

13. Based upon my training and experience, as well as conversations with other law enforcement officers and computer forensic examiners, I know that these electronic "chat logs" often have great evidentiary value in child pornography investigations, as they record communication in transcript form, show the date and time of such communication, and also may show the dates and times when images of child pornography were traded over the Internet. In addition to electronic communication, a computer user's internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such

information is often maintained on a computer for long periods of time until overwritten by other data.

### **P2P FILE-SHARING IS A GROWING PHENOMENON**

14. A growing phenomenon on the Internet is peer-to-peer file-sharing (P2P). P2P file sharing is a method of communication available to Internet users through the use of special software. The software is designed to allow users to trade digital files through a worldwide network that is formed by linking computers. There are several different software applications that be used to access these networks, but these applications operate in essentially the same manner.

15. To access the P2P networks, a user first obtains the P2P software, which can be downloaded from the Internet. This software is used exclusively for the purpose of sharing digital files. Once the P2P software is installed on a computer, the user is directed to specify a "shared" folder. All files placed in that user's designated "shared" folder are available to anyone on the world wide network for download. Most P2P software gives each user a rating based on the number of files he/she is contributing to the network. This rating affects the user's ability to download files. The more files a user is sharing, the great his/her ability tis to download files. This rating system is intended to encourage users to "share" their files, thus propagating the P2P network. A user, however is not required to share files in order to utilize the P2P network.

16. A user obtains files by conducting keyword searches of the P2P network. When a user initially logs onto the P2P network, a list of the files that the user is sharing is transmitted to the network. The P2P software then matches files in these file lists to keyword search requests from other users. A user seeking to download files simply conducts a keyword search. The results of the keyword search are displayed and the user then selects the file(s) which he/she would like

to download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) hosting the file. Once a file had been downloaded, it is stored in an area previously designated by the user and will remain there until moved or deleted. The majority of the P2P software applications retain logs of each download event.

17. A person interested in sharing child pornography with others via a P2P network, needs only to place those files in his/her "shared" folder(s). Those files are then available to all users of the P2P network for download, regardless of their physical location.

18. A person interested in obtaining child pornography can open the P2P application on his/her computer and conduct a keyword search for files using a search term, such as "preteen sex." The keyword search would return results of files being shared on the P2P network that match the term "preteen sex." The user can then select a file(s) from the search results and the selected file(s) can be downloaded directly from the computer(s) sharing the file(s).

19. The computers that are linked together to form the P2P network are located throughout the world. Therefore, the P2P network operates in interstate and foreign commerce.

20. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel (i.e. the user can download more than one file at a time). In addition, a user may download parts of one file from more than one source computer at a time. For example, a user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this process is that it reduces the time it takes to obtain a file(s). A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. An IP address is expressed as four numbers separated by decimals. Each number, which can range from 0 to 256, is unique to a particular internet connection during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

21. Even though the P2P network links together computers all over the world and users can download files, it is not possible for one user to send or upload a file to another user of the P2P network. The software is designed only to allow files to be downloaded that have been selected. One does not have the ability to send files from his/her computer to another's computer without their permission or knowledge. Therefore, it is not possible for one user to send or upload child pornography files to another user's computer without his/her active participation.

22. P2P networks, such as the one utilized in this investigation, can be accessed through applications on cellular phones.

23. Third-party software is available to identify the IP address of the P2P computer sending the file. Such software monitors and logs Internet and local network traffic.

24. Gnutella is a P2P network. Users of the Gnutella network share content on the network by using one of several client software programs capable of using the Gnutella network rules and language (protocols).

25. "Shareaza LE" is available to law enforcement officers and is a modified P2P software program that law enforcement officers use to work undercover operations to identify IP addresses that share child pornography. While using this software, law enforcement officers can connect to the Gnutella, Gnutella 2, eDonkey, and Ares P2P networks. Shareaza LE allows law enforcement to establish a direct connection with other host computers on these P2P networks and conduct a sole-source download (downloading all pieces of a single file from the same peer) in lieu of "swarming" (downloading different pieces of a single file from multiple peers). This software also identifies and captures the Internet Protocol (IP) address and Globally Unique Identifiers (GUIDs) transmitted by the computers with which it establishes a connection and downloads files. A GUID is a reference number used as an identifier in computer software.

Additionally, the software allows law enforcement officers to view the hash value in the file listings returning in both the "browse" function and "file query" function on the P2P networks.

26. When computers on the Gnutella, Gnutella 2, and the eDonkey networks communicate they transmit identifying information about themselves. One such piece of information that is obtainable is the IP address of the computer on the other end. Two other pieces of information obtainable in the communication streams are the type of software and the GUID. When a person installs a P2P program on a computer, a mathematical procedure (i.e. a hash function) for that computer calculates a GUID based on the computer's configuration, Network Interface Card (NIC), and hardware. In many cases an encryption file is created and tied to that GUID to prevent anyone else from using that same GUID on the system. The very nature of the Gnutella, Gnutella 2, and the eDonkey networks requires computers to have a unique GUID to ensure correct communications on the network.

27. When comparing GUIDs, it can be determined with a high degree of certainty that two different IP addresses that are associated with the GUID are associated with the same computer.

28. There are automated tools available to law enforcement that can be used to automate the search process for the aforementioned search terms and then can be used to identify, by IP address, those users offering to trade files that have those terms in them. The returned lists of IP addresses offering those files for trade can be scanned specifically for digital signatures of known or suspected child pornography by those same automated tools and the information can be recorded and examined by jurisdictions across the country. One such tool, the Child Protection System (CPS) was utilized by the NM ICAC for this investigation.

29. The Gnutella networks have a built-in functionality to insure precise file matching. On the Gnutella network, precise file matching is don't through the use of SHA-1 digital signatures. The method used by the Gnutella P2P network involves a file encryption method called Secure Hash Algorithm version 1, or more commonly known as SHA-1. A SHA-1 value can be likened to DNA. It is, in essence, a mathematical fingerprint of a computer file that will remain the same for an unchanged file no matter where the file is found, on which computer the file is located, or what the file is named. In this investigation, SHA-1 values were used by the CPS database, to identify files that are known child pornography files.

**PEER-TO-PEER (P2P) FILE SHARING AND INVESTIGATIONS**  
**BY UNDERCOVER LAW ENFORCEMENT OFFICERS**

30. On July 27, 2018, NM ICAC Special Agent Owen Pena was conducting an online investigation and examined the records contained in the Child Protection System (CPS) database, specifically focusing on IP addresses/GUIDs believed to be in New Mexico and offering to participate in the distribution of files containing child sexual exploitation. He noted one IP address that was associated with five GUIDs which all contained SHA1 Hash Values that contained files indicative of child pornography. He noted that that IP address (146.5.17.100) had been logged in the CPS from January 24, 2018, through February 23, 2018. The CPS servers reported that this IP address was located at the National Solar Observatory (NSO) in Sunspot, New Mexico.

31. While examining the records contained in the CPS database, SA Pena noted that another IP address (146.5.17.47) was associated with two GUIDs which all contained SHA1 Hash Values that contained files indicative of child pornography. He noted that IP address 146.5.17.47 had been logged in the CPS from April 3, 2018, through June 11, 2018. The CPS servers reported that this IP address was located at the National Solar Observatory (NSO) in Sunspot, New Mexico.

32. While continuing to examine the records contained in the CPS database, SA Pena noted that a third IP address (146.5.17.80) was associated with one GUID which contained SHA1 Hash Values that contained files indicative of child pornography. He noted that IP address 146.5.17.80 had been logged in the CPS from July 4, 2018, through July 12, 2018. The CPS servers reported that this IP address was located at the National Solar Observatory (NSO) in Sunspot, New Mexico.

33. SA Pena then queried MaxMind.com for the above three IP addresses, and noted that all three IP addresses were registered to the National Solar Observatory (NSO) through Tularosa Communications. SA Pena contacted Tularosa Communications and learned that this block of IP addresses belongs solely to the National Solar Observatory in Sunspot, NM. Furthermore, SA Pena was advised that the contact person for NSO is John Doherty.

34. On July 31, 2018, SA Pena contacted John Doherty and advised him of the fact that multiple files containing child pornography had been seen coming from the IP addresses which belonged to the NSO. SA Pena was referred to the Director of the NSO. On August 1, 2018, SA Pena contacted the Director of the NSO, who advised SA Pena that he had ordered that the local public network at that site be disabled, as a precautionary measure. The Director arranged for a conference call on August 2, 2018, which included himself, SA Pena, NSO's IT Manager, and Valen Schnader, Chief of Staff for the Association of Universities for Research in Astronomy (AURA). The NSO at Sunspot, NM is managed by AURA, under a cooperative agreement with the National Science Foundation. The National Science Foundation funds the research conducted at the facility and AURA manages the facility. During the conference call on August 2, 2018, it was decided that the public network site would be recreated or re-opened, in an attempt to allow

the subject to gain access to the internet, for the purpose of monitoring activity and definitely identifying the subject.

35. Immediately after "re-opening" the network on August 2, 2018, NSO's IT Manager could detect inbound traffic to the specific port which had been blocked, with a newly assigned IP address (146.5.17.84). The IT Manager advised SA Pena that the MAC Address for the device accessing the IP address was: 00:26:82:1b:16:f5, and that the Operating System was Windows XP. Later, the IT Manager advised SA Pena that he was able to trace the host computer with the above MAC Address to a wireless access point (AP42100) that is located inside the Dunn Solar Telescope, in the hallway with the doors to the offices. The IT Manager also advised SA Pena that the specific access point does not serve the housing units located at Sunspot, NM.

36. On August 6, 2018, NM ICAC Special Agent Jay Ratliff, while working in an undercover capacity utilizing P2P software program Shareaza 2.7.9.0, received a browse of a child pornography file from IP Address: 146.5.17.84 with GUID: 078C2CD8305A5444B488518F8DC6FCEB. That is the same IP address which was assigned to the NSO on August 2, 2018, upon re-opening of the network by the NSO IT Manager. Furthermore, the above GUID is consistent with a child pornography file. In fact, during the time period between August 2, 2018, at approximately 3:00 p.m. MDT and August 6, 2018 at approximately 3:00 p.m. MDT, the CPS database records showed that the above IP address had been offering to participate in the distribution of files containing child pornography. During the four day time period, the GUID record showed Hash Values for over 200 files of known child pornography.

37. SA Pena provided the other three IP addresses to SA Ratliff, associated with the NSO, and SA Ratliff reviewed his undercover investigative activity for the previous months. SA Ratliff noted that on February 23, 2018, while working in an undercover capacity utilizing the P2P software program Shareaza 2.7.9.0, he had connected to IP address 146.5.17.100 and had received two partial files from that IP address, which were consistent with child pornography, and with the following GUID: 11B2275E1D80CD4BA95C5D876254D03C. That same GUID was captured by the CPS system as being offered by a host computer at the IP address 146.5.17.100 on February 23, 2018, with over 100 files whose SHA-1 Hash Values and filenames are consistent with child pornography.

38. After learning that the NSO buildings and research are funded by the National Science Foundation, and that the land upon which they sit is owned by the U.S. National Park Service, SA Pena contacted your affiant to arrange for referral of the case to the FBI.

39. On August 10, 2018, your affiant contacted Mr. Schnader and began a dialog with him concerning individuals with access to the Observatory, as well as which individuals were present at different times of the day.

40. On August 14, 2018, your affiant analyzed the results from the CPS GUID records for the IP addresses 146.5.17.100, 146.5.17.47, 146.5.17.80, and 146.5.17.84. During the time period from August 2, 2018, at 3:00 p.m. EDT through August 4, 2018, at 5:26 p.m. EDT (over 26 hours). At 5:26 p.m. EDT on August 4, 2018, the host computer was disconnected from the network and did not connect to the network again until 6:02 p.m. EDT. For nine of the next 11 days, the host computer was connected from approximately 6:00 p.m. EDT every evening until approximately 5:30 p.m. EDT the following day, then disconnected for approximately 30 minutes

before being reconnected again. A similar pattern was observed from February of 2018 until August 14 of 2018, with the connection times increasing in proximity to the 6:00 p.m. mean. It is therefore most likely that the individual downloading and distributing child pornography was present within the facility between approximately 5:30 p.m. and 6 p.m. on an almost daily basis.

41. On August 21, 2018, your affiant received records from Special Agent Pena, showing that the host device had not been connected to the wireless internet using IP Address 146.5.17.84 from Wednesday, August 15<sup>th</sup> at 2:42 p.m. EDT until Monday, August 20<sup>th</sup> at 3:16 p.m. EDT. On August 20, 2018 at 3:16 p.m. EDT a host device had been connected to the internet using IP Address: 146.5.17.84.

42. On August 21, 2018, Mr. Schnader contacted your affiant and advised that the Chief Observer at the National Solar Observatory in Sunspot had notified his supervisor that he had found a laptop computer running in an empty office. He further reported to his supervisor that he had seen the same laptop computer secreted and running in two other offices over the past several months. The first time he picked up the computer, he described the contents on the desk top as "not good." This time when he found the laptop computer, he checked the IP Address, and reported it to his supervisor as "146.5.17.84." Mr. Schnader provided contact information for the Chief Observer, and notified him that your affiant would contact him momentarily.

43. On August 21, 2018, your affiant interviewed the Chief Observer telephonically. Upon learning that the Chief Observer had found the laptop computer running several months ago, in a different location, and had at that time seen an image that was consistent with child pornography, your affiant requested that the Chief Observer lock down the facility and remain there until your affiant could seize the device.

44. On August 21, 2018, your affiant arrived at the National Solar Observatory and interviewed the Chief Observer in person. Thereafter, your affiant photographed the room in which the Lenovo laptop computer was plugged in and running. Your affiant also observed and photographed the room in which the Lenovo laptop computer had been plugged in and running several months earlier (the day on which the Chief Observer had seen an image consistent with child pornography). Your affiant noted that the Lenovo laptop computer was an IdeaPad with a Windows XP logo near the keyboard. The program "Shareaza" was on the screen, and your affiant photographed the computer screen in place prior to seizing the computer. After seizing the computer, your affiant transported it to the FBI Office in Las Cruces, New Mexico. It is currently located in the temporary evidence room located within the secure FBI Office.

45. Further information learned from the Chief Observer on August 21, 2018, indicates that he had originally found the Lenovo laptop computer several months ago, in an office used only two or three times a year by a retired professor who now has Emeritus status. The professor asked the Chief Observer to examine his desktop computer within his office, as it was not working properly. Under the desk, in the space between the desktop computer's central processing unit (CPU) and the wall, the Chief Observer found a Lenovo laptop computer plugged in and running. When he opened the laptop computer, he saw an image of a naked adult woman, which rapidly changed to an image which the Chief Observer described as being a female child with her face covered with a mask. The Chief Observer assumed the laptop computer belonged to one of the New Mexico State University (NMSU) students who occasionally conducted research at the Observatory. The Chief Observer was distracted by an urgent matter within the facility, shut the computer, and did not report the incident.

46. Several weeks later, the Chief Observer was asked by another Emeritus professor to look for some software disks. This Emeritus professor has relocated to Montana and has not been in the Observatory (or that office) for many months. The Chief Observer saw the Lenovo laptop computer secreted in the office, plugged in, and running. Again, he assumed the laptop computer was being used by an NMSU student who knew the office was rarely used.

47. On August 21, 2018, the Chief Observer walked into an office that has been unassigned for several months, and was scheduled to be assigned in the future to an individual who had recently been hired and was scheduled to arrive in September of 2018. The Chief Observer saw the same Lenovo laptop computer secreted in the corner of the office, plugged in and running. He queried the IP address and noted that the computer was running the Windows XP operating system. The Chief Observer realized that the laptop computer did not belong to one of the NMSU students, because no students had been in the Observatory for at least ten days. The Chief Observer also noted that only three individuals had been in the Observatory over the past 36 hours: himself, Chris Mitchell, and Joshua Cope. All three of those individuals have a key to the building and also have the code to access the building. They are all free to come and go, and lock up the building.

48. Chris Mitchell began his employment at the Observatory in May of 2018. He did not have access to the Observatory during the time period from January of 2018 until May of 2018, when the wireless Internet signal was used to download files consistent with child pornography.

49. Joshua Cope began providing janitorial services at the Observatory approximately one year ago. He generally arrived to clean at approximately 2 p.m. and stayed for a couple of hours. On numerous occasions, when the Chief Observer had departed for the day at

approximately 3 p.m., Cope had offered to lock the facility when he departed. Cope has a key to the building and unlimited access to the building, and is familiar with which offices are used only a handful of times a year. When he is not going to be available to clean, his parents (who have the cleaning contract for both the Apache Point Observatory and the Sunspot Observatory) notify the Chief Observer via email. In fact, Cope attended a wedding with his parents on the East Coast, and was not present in the Observatory from Thursday afternoon until Monday afternoon (August 15, 2018 until August 20, 2018).

50. On August 21, 2018, SA Pena provided the GUID records for IP Address 146.5.17.84. A device connected to the IP address and utilized Shareaza P2P software to offer file names which were consistent with known child pornography, and SHA1 Hash Values which were consistent with known child pornography, at approximately 3:16 p.m. EDT on August 20, 2018. Prior to that date and time, the last time a device was connected to IP Address 146.5.17.84, utilizing Shareaza P2P software to offer child pornography for distribution, was August 15, 2018 at approximately 2:42 p.m. EDT.

51. On August 22, 2018, SA Pena provided the GUID records for IP Address 146.5.17.84. The GUID records showed that the device was connected and utilizing the Shareaza software until approximately the time in which your affiant seized the laptop computer and removed it from the facility in which it had been accessing the above IP address.

52. On August 24, 2018, your affiant conducted another telephonic interview with the Chief Observer. He advised that Joshua Cope had arrived the morning following the seizure of the laptop computer (August 22, 2018), and the Chief Observer had seen Cope exiting the office in which the computer had been located the day before. Cope approached the Chief Observer and

stated that he was missing some cleaning supplies which he had left in the office, and asked if anyone had been in the office. The Chief Observer advised your affiant that he had located the Lenovo laptop computer next to a box of cleaning supplies on the day in which the computer was seized. The Chief Observer advised that there was no reason for anyone to be in the office, as the assigned person had not been there in many months. Cope then stated that he needed to clean the office next door, and needed to gain access to the office, which had been locked by the Chief Observer after Agents departed the observatory. This is the same office in which the Chief Observer had previously found the small Lenovo laptop computer secreted.

53. Later in the day, Cope reported that he thought someone had been entering the Observatory at night, in order to steal the wireless Internet service. He also stated that he was concerned that security was so lax, as in January of 2018 he had seen a man parked in a truck outside of the Observatory, handling an item that appeared to be a black book. Cope then stated that someone had stolen five rolls of toilet paper from the facility. The Chief Observer stated that he would look into the matter.

54. The following day (August 23, 2018), Cope stated that he was tired of people taking his things, and that he was no longer going to bring any personal items into the Observatory. He stated that many people knew the passcode into the facility, and the code should be changed. He then stated to the Chief Observer words to the effect of, "I should be able to throw a laptop down in a room and not have to worry about someone stealing it." The Chief Observer described Cope's actions as being frantic, and noted that Cope had continued to approach him throughout the day with questions and comments about missing items and lax security, which Cope had not discussed in his previous year of cleaning the Observatory.

### **CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS**

55. Based on my experience, training, and conversations with other experienced agents who investigate cases involving the sexual exploitation of children, I know that certain common characteristics are often present in individuals who collect child pornography. I have observed and/or learned about the reliability of these commonalities and conclusions involving individuals, who collect, produce and trade images of child pornography. Based upon my training and experience, and conversations with other experienced Agents in the area of investigating cases involving sexual exploitation of children, I know that the following traits and characteristics are often present in individuals who collect child pornography:

a. Many individuals who traffic in and trade images of child pornography also collect child pornography. Many individuals who collect child pornography have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by sexually explicit depictions of children.

b. Many individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. Many of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. Many individuals who collect child pornography often seek out like minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and

associated behavior. The different Internet based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, email, email groups, bulletin boards, Internet Relay Chat Rooms (IRC), newsgroups, instant messaging, and other similar vehicles.

d. Many individuals who collect child pornography maintain books, magazines, newspapers and other writings (which may be written by the collector), in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for the illicit behavior and desires. Such individuals often do not destroy these materials because of the psychological support that they provide.

e. Many individuals who collect child pornography often collect, read, copy or maintain names, addresses (including email addresses), phone numbers, or lists of person who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. Many individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect them from discovery, theft, or damage. These individuals view their sexually explicit materials as prized and valuable materials, even as commodities to be traded with other likeminded individuals over the Internet. As such, they tend to maintain or "hoard" their visual depictions of child pornography for long periods of time in the privacy and security of their homes or other secure locations. Based on my

training and experience, as well as my conversations with other experienced law enforcement officers, I know that individuals who possess, receive, and/or distribute child pornography by computer using the internet often maintain and/or possess the items listed in Attachment B.

56. Individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage to their collection of illicit materials. The known desire of such individuals to retain child pornography together with the sense of security afforded by using computers, provides probable cause to believe that computer images, especially child pornography and erotic nudity involving minors, will be retained by collector indefinitely. These individuals may protect their illicit materials by passwords, encryption, and other security measures, save it on movable media such as CDs, DVDs, flash memory, thumb drives, and removable hard drives, which can be very small in size, including as small as a postage stamp, and easily secreted, or send it to third party image storage sites via the Internet.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

57. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with

deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

58. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

59. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

## **SEARCH METHODOLOGY TO BE EMPLOYED**

60. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

**BACKGROUND OF INVESTIGATION AND  
FACTS ESTABLISHING PROBABLE CAUSE**


61. The FBI is investigating Joshua Cope as a suspect for using one or more computers and computer media at this facility to commit violations of Title 18, United States Code, Sections 2252 and 2252A, which prohibit mailing, transportation, shipment, receipt, possession and access with intent to view, in interstate or foreign commerce by any means; including by computer, any child pornography.

62. Based on the investigation, FBI now believes that Joshua Cope, who works as a janitor inside the Dunn Solar Telescope (DST) Observatory in Sunspot, New Mexico, is the user of the computer which was being used to access the wireless Internet signal, and to download and distribute child pornography. This is based on the following facts: 1) The wireless Internet signal being used to access and distribute child pornography is contained within the DST Observatory; (2) the wireless Internet signal does not reach the housing units near the DST Observatory; (3) there are only two individuals who access the DST Observatory after dusk and before dawn; (4) the activity began months after Joshua Cope gained access to the DST Observatory and months prior to the time when Chris Mitchell gained access to the DST Observatory; (5) the other individuals with keys to the building and knowledge of the access code are there only a couple of times per year, and did not have access to the DST Observatory from August 20, 2018 until August 21, 2018; (6) Joshua Cope was not present in the DST Observatory during the five day period in which SA Pena queried the ICAC secure website for the recent history of the user using the IP address 146.5.17.84, and noted that the user was not actively offering to share files consistent with child pornography; and Joshua Cope was present in the DST Observatory during the days/nights in which the host device was connected to the IP addresses within the facility, and actively offering to share files consistent with child pornography.

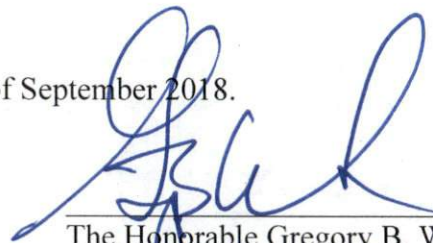
### CONCLUSION

63. Based on my training and experience and the facts set forth above, I have probable cause to believe that Joshua Cope is involved in the possession and distribution of child pornography, in violation 18 U.S.C. §§ 2252 and 2252A. Additionally, I have probable cause to believe that evidence of criminal offenses, namely, violations of 18 U.S.C. §§ 2252 and 2252A, is located in the device listed in Attachment B to this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

64. Accordingly, I respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

  
\_\_\_\_\_  
Lisa Kite Hill  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn before me this 6th day of September 2018.

  
\_\_\_\_\_  
The Honorable Gregory B. Wormuth  
United States Magistrate Judge